NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 6-20

Issue Date: 31 March 2014
Revised: 8 November 2016

(U) SECOND PARTY ACCESS TO NSA/CSS TS/SCI CLASSIFIED INFORMATION SYSTEMS

(U) PURPOSE AND SCOPE

(U) This policy defines processes and procedures for *Second Party* access to NSA/CSS classified *information systems (ISs)*. This policy applies to all *United States Cryptologic System (USCS)* organizations that sponsor *Second Party integrees*, *USCS personnel* who initiate or approve requests for Second Party personnel access to U.S. classified intelligence and cryptographic information, and USCS personnel who implement Second Party personnel and systems access to any NSA/CSS classified ISs.

RICHARD H. LEDGETT, JR.
Acting Director, NSA

Endorsed by
Associate Director for Policy

(U) Encl:
Annex – Second Party Access Information

(U) DISTRIBUTION:
TS23
DJ1
DJ2 (Vital Records)
DJ6 (Archives)

(U) This Policy 6-20 supersedes NSA/CSS Policy 6-20 dated 2 July 2007.
(U) OPI: NSA/CSS IT Policy, TS23, 303-1896s.

(U) This Policy 6-20 supersedes NSA/CSS Policy 6-20 dated 2 July 2007. The Chief, Policy approved an administrative update on 26 February 2015 to reflect new guidance on limited administrator access, align the definition of Second Party Integree with NSA/CSS Policy 1-13, and make other administrative changes. The Chief, Policy approved an administrative update on 2 November 2015 to update the definition "Authorizing Official." The Chief, Strategy, Plans, and Policy approved an administrative update on 8 November 2016 to enable qualified Second Party Liaison officers to routinely obtain direct access to NSANet. The administrative update also clarifies the terms 'second party personnel' and 'second party integrees', and makes their use more consistent; improves accuracy in specifying NSANet access type; clarifies a Second Party and Multinational Affairs Division (P523) responsibility; updates definitions; and makes minor administrative updates.
(U) OPI: Technology Policy, P12T, 717-0220s.
(U) No section of this document shall be released without approval from the Office of Policy (P12).

(b)(3)-P.L. 86-36

(U) POLICY

1. (U) It is the policy of NSA/CSS to share with Second Party *Cryptologic* partners all information relevant to the arrangements outlined in "U.K.-U.S. Communications Intelligence Agreement (UKUSA)" (Reference a) and subsequent bilateral understandings with each Second Party partner as outlined in [redacted] (Reference b), NSA/GCHQ/DSD/CSE/GCSB "Second Party Intranet Connection MOU" (Reference c), and [redacted] (Reference d).

2. (U) Second Party system access shall be provided in accordance with the requirements specified in Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management" (Reference e).

3. (U//~~FOUO~~) Second Party Personnel may not perform information technology (IT) systems administrative functions or be granted *privileged access* on NSA/CSS IT systems, with the exception of limited administrative privileges in direct support of mission requirements (i.e., a virtual machine or workstation the administrative access to which is expressly required for mission purposes).

4. (U) Second Party system connection and access policy agreements between the USCS *information steward* and each Second Party country shall be established in a Memorandum of Understanding (MOU). Documents will be maintained and posted by Office of Policy (P12) on *NSA/CSS Classified Network (NSANet)*.

5. (U) Second Party integrees and Second Party Liaison officers who meet the access requirements in this policy shall routinely be given direct access to NSA/CSS ISs via individual NSA/CSS accounts.

6. (U) *Second Party Headquarters Personnel* shall routinely access NSA/CSS classified ISs indirectly via the Second Party proxy server.

7. (U//~~FOUO~~) Second Party Personnel who are not eligible for direct access and whose requirements cannot be accommodated via the proxy server may request an *exception* to obtain direct access to NSA/CSS IS via an individual NSA/CSS account.

8. (U) All requests for Second Party direct access to NSA/CSS ISs shall be approved by the Second Party authority with parallel responsibility to NSA/CSS mission or mission-support information (e.g., signals intelligence (SIGINT), information assurance (IA), research) before presentation to NSA/CSS for consideration. Second Party requests for individual NSANet accounts must be authorized in writing by the responsible Second Party authority.

9. (U) All Second Party personnel who require direct access to classified NSA/CSS ISs for the performance of a SIGINT production mission must also follow the guidance within:

a. (U) SIGINT Directorate (SID) Management Directive 421, "United States SIGINT System Database Access" (Reference f);

b. (U) SID Management Directive 422, "USSS Mission Delegation" (Reference g); and

c. (U) SID Management Directive 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel" (Reference h).

10. (U) For direct access to NSA/CSS classified ISs, eligible Second Party personnel must be appropriately cleared and approved by the Second Party and Multinational Affairs Division (P523). In addition, Second Party integrees must be sponsored by a *Global Enterprise Leader*.

11. (U) All Second Party personnel who have obtained an NSANet user account shall complete NSA/CSS Information Assurance training (e.g., OIAC1180, "Cyber Awareness Challenge," OVSC1000, "Intelligence Oversight Training") prior to access and yearly thereafter.

12. (U) All Second Party personnel with direct access to NSANet must obtain and use Cryptologic Agencies Domain certificates if possessing citizenship in a Five Eyes country. Additional information can be found on the NSA Corporate Public Key Infrastructure (PKI) Information Page;

13. (U) All Second Party personnel with direct access to NSA/CSS ISs shall be subject to all NSA/CSS Information Technology policies and procedures.

14. (U) The citizenship of all Second Party personnel given individual NSANet accounts shall be uniquely identified in the NSA/CSS Directory Service (i.e., SEARCHLIGHT) in order to provide strong network and ISs access control.

15. (U) Second Party personnel with individual NSANet accounts may be directly connected only to those NSA/CSS classified ISs required to perform sponsored functions. For integrees, the sponsoring organization shall be the authority to identify what is required and shall

(b)(3)-P.L. 86-36

have a process to account for the systems and information accessed by the integree. The *System Security Plans (SSPs)* of all systems identified for Second Party integree access must be updated to reflect this access.

16. (U//~~FOUO~~)

17. (U//~~FOUO~~)

18. (U//~~FOUO~~)

19. (U) All Second Party access to non-NSA/CSS information on NSA/CSS ISs shall be controlled in accordance with an agreement with the information steward or procedures established by the information steward. Access to ISs containing non-NSA/CSS information must be approved, in writing, by the originating agency of the data, and documented in the SSP.

20. (U) Under no circumstances will any Second Party Personnel to include partners, liaison officers or integrees be provided direct access to NSA/CSS ISs that are used to generate, produce, or electronically track and distribute U.S.-only keying materials, or *Nuclear Command and Control Information Assurance Materials (NCCIM)*.

21. (U) All Second Party personnel who no longer require access to NSA/CSS classified ISs shall have their access terminated upon completion of those specific official duties. This access is not transferable. If Second Party personnel require access in a new position, they must reapply for the access based on their new duties.

(U) PROCEDURES

22. (U) **Procedures for Second Party Indirect Access to NSA/CSS Information Systems via Second Party Proxy Server**:

a. (U) Written authorization is not required for Second Party personnel access to NSA/CSS ISs via Second Party proxy servers; and

b. (U) Second Party personnel are not required to register with NSA/CSS before accessing NSA/CSS resources via Second Party proxy servers.

23. (U) **Procedures for Second Party Direct Access to NSA/CSS Information Systems**: As noted above, Second Party liaison officers and integrees at NSA/CSS will be routinely sponsored for accounts on NSANet. Other Second Party personnel may be approved for such access on a case-by-case basis. The following procedures, therefore, apply to all Second Party liaison officers and integrees and to specially approved other Second Party personnel, as noted below. USCS organizations that wish to sponsor Second Party personnel for direct access to NSA/CSS ISs shall:

a. (U) Acquire and maintain, for each Second Party candidate, a record of the information specified within the Annex;

b. (U) For integrees only, prepare a formal requirements statement describing the systems, information, and services required for the Second Party individual(s) to perform official NSA/CSS-sanctioned duties; and

c. (U) Forward the sponsor and candidate information described in the above subparagraphs a (and b when applicable), to the Second Party and Multinational Affairs Division (P523) for approval and subsequent transferal to the Office of Security and Counterintelligence (A5) for NSA/CSS Personnel Security System Database (e.g., CONCERTO) record development. *Service Partners* will forward sponsor and candidate information through their respective cryptologic offices at *NSAW (NSA/CSS Washington)*.

24. (U) **Exceptions to Access Policy**: Organizations requesting an exception to this policy or its annex shall coordinate a written request with their Information System Security Officer (ISSO). Requests will be reviewed by the Information System Security Manager (ISSM) and Second Party and Multinational Affairs Division (P523), prior to submission to the NSA/CSS *Authorizing Official (AO)* for decision.

(U) RESPONSIBILITIES

25. (U) USCS organizations sponsoring Second Party personnel for direct NSA/CSS IS access and NSA/CSS accounts shall:

a. (U) Verify that formal access requirements, including requirements for ISs, data, and services, are defined for Second Party personnel and appropriately coordinated with other organizations when access to data from multiple information stewards is required;

b. (U) Ensure that access requests are consistent with requirements for performance of official NSA/CSS-sanctioned duties;

c. (U) Advise the Second Party and Multinational Affairs Division (P523) and Service Cryptologic Offices (if applicable) of the formal access request requirement and obtain Second Party and Multinational Affairs Division (P523) concurrence;

d. (U) Confirm that the sponsored Second Party personnel are registered in the NSA/CSS Personnel Security System Database (i.e., CONCERTO) and the NSA/CSS Directory Service (i.e., SEARCHLIGHT);

e. (U) Verify that the Capabilities Directorate (Y) has approved all connectivity and access mechanisms before granting Second Party data access;

f. (U) Notify the Second Party and Multinational Affairs Division (P523), respective Service Cryptologic Offices (if applicable), the ISSO, the manager of the controlled interface, and system administrators when Second Party personnel access is no longer required;

g. (U) Be accountable for Second Party direct system access. Report any suspected anomalies, known or suspected unauthorized access, or problems associated with sponsored Second Party access in accordance with NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents" (Reference k); and

h. (U) Report anomalous activity and incidents to the Office of Security and Counterintelligence (A5) and the Capabilities Directorate (Y) for appropriate investigation.

26. (U) The Capabilities Directorate (Y) shall:

a. (U) Establish and maintain central oversight and accountability for Second Party access through the controlled interface and its separate services; and

b. (U) Provide technical guidance on quality, technical risk assessment, and procedures for connecting any Second Party personnel to NSA/CSS classified ISs.

27. (U) The Second Party and Multinational Affairs Division (P523) shall:

a. (U//~~FOUO~~) Ensure that appropriate NSA/CSS elements such as Capabilities Directorate (Y) and the Office of Security and Counterintelligence (A5) receive information relative to the arrivals and departures of Second Party persons sponsored for Direct NSA/CSS IS access/NSANet accounts. This will enable Standard Identification (sid) creation, SEARCHLIGHT record/account development/deletion as appropriate, and PKI approvals. These database records will form the core information set to enable NSA/CSS to satisfy internal, Department of Defense, and Intelligence Community requirements for secure and discrete information access and exchange; and

b. (U//~~FOUO~~) Approve the creation of NSANET accounts for Second Party Personnel eligible for direct access.

28. (U) The Security and Counterintelligence (A5) shall:

a. (U//~~FOUO~~) Receive and review approved requests from the Second Party and Multinational Affairs Division (P523) for Direct NSA/CSS IS access/NSANet accounts by Second Party persons and develop and maintain appropriate security records (e.g., CONCERTO) and convey sid and record data to Capabilities Directorate (Y) directorate systems that support and mediate such access (e.g., SEARCHLIGHT, CASPORT); and

b. (U) Investigate anomalous activity and incidents associated with Second Party access to NSA/CSS classified ISs in coordination with the NSA/CSS Capabilities Directorate (Y).

29. (U) The NSA/CSS Headquarters and Field ISSMs shall work with USCS organizations sponsoring Second Party integrees to ensure that information system security issues are addressed and resolved.

30. (U) NSA/CSS AO shall review requests for exceptions to this policy and render decisions.

31. (U) Privileged access users and ISSOs shall:

a. (U) Notify USCS system users when Second Party personnel have accounts on an IS or local area network;

b. (U//~~FOUO~~) Confirm that Second Party accounts are set up correctly and removed upon completion of specified official duties per NSA/CSS Policy 6-8, "Information System User and Supervisor Security Responsibilities" (Reference l);

c. (U) Report any anomalous activities in accordance with Reference k and assist, as necessary, in any investigations or analyses of such anomalies; and

d. (U) Assist in the enforcement of the data access procedures established by the information steward's or sponsor's policies and directives.

(U) REFERENCES

32. (U) References:

a. (U) U.K.-U.S. Communications Intelligence Agreement (UKUSA) dated 5 March 1946.

b. (U) [redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

c. (U) NSA/GCHQ/DSD/CSE/GCSB Second Party Intranet Connection MOU dated 27 October 1998.

d. (U) [redacted]

e. (U) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management," dated 21 July 2015.

f. (U) SID Management Directive (SMD) 421, "United States SIGINT System Database Access," revised 25 March 2008.

g. (U) SID Management Directive (SMD) 422, "USSS Mission Delegation," revised 15 April 2008.

h. (U) SID Management Directive (SMD) 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel," revised 28 December 2013.

i. (U) SID Delegation of Approval Authorities Matrix dated 20 November 2014.

j. (U) IAD Management Directive 128, "Approval and Release of Technical IA Information," dated 22 June 2012.

k. (U) NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents," dated 4 December 2012 and revised 14 November 2014.

l. (U) NSA/CSS Policy 6-8, "Information System User and Supervisor Security Responsibilities," dated 1 August 2016.

(U) DEFINITIONS

33. (U) Authorizing Official (AO) – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Source: CNSS Instruction (CNSSI) 4009 dated 6 April 2015)

34. (U) Cryptologic – Related to the collection and/or exploitation of foreign communications and non-communications emitters, known as SIGINT; and solutions, products, and services to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems, known as Information Assurance (IA). (Source: NSA/CSS Corporate Policy Glossary)

35. (U) Exception – Indicates that an implementation of one or more security requirements is temporarily postponed and that satisfactory substitutes for the requirement(s)

may be used for a specified period of time. This is in contrast to a waiver that implies a security requirement has been set aside and need not be implemented at all.

36. (U) Global Enterprise Leaders – NSA/CSS Directors, the NSA Chief of Staff, SCC Commanders, Senior NSA/CSS Representatives, and the military commanders/civilian chiefs of NSA/CSS Extended Enterprise sites. (Source: NSA/CSS Corporate Policy Glossary)

37. (U) Information System (IS) – Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition/collection, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. IS examples are: stand-alone systems, Local Area Networks, supercomputers, process control computers that perform special purpose computing functions (e.g., Supervisory Control and Data Acquisition, other Industrial Control Systems, embedded computer systems), and the communications networks that disseminate information. (Source: NSA/CSS Corporate Policy Glossary)

38. (U) Information Steward – An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. (Source: CNSSI 4009)

39. (U) NSA/CSS Classified Network (NSANet) – The TS/SCI information technology that enables the NSA/CSS to conduct its cryptologic missions, including signals intelligence and information assurance, and to support cyber operations missions in concert with the NSA/CSS Global Cryptologic Enterprise. Several conditions must be satisfied before an IS can be considered part of the NSANet. In particular each and every IS that is part of the NSANet must have a registered unique IP address; must be located in a SCIF [sensitive compartmented information facility] accredited by NSA/CSS or another IC agency or a Second Party Partner and approved by NSA/CSS to conduct NSA/CSS activities; and be under NSA/CSS authority. (Source: NSA/CSS Corporate Policy Glossary)

40. (U) NSA/CSS Washington (NSAW) – NSA/CSS facilities at the Fort Meade, Friendship Annex (FANX), and associated campuses [Finksburg, Kent Island, and all leased facilities in the Baltimore/Washington metropolitan area]. (Source: NSA/CSS Corporate Policy Glossary)

41. (U//~~FOUO~~) Nuclear Command and Control IA Material (NCCIM) – IA materials used in safeguarding and validating the use of nuclear weapons and weapon systems. These include, but are not limited to materials used in authentication, encoding/decoding, and/or locking/unlocking functions associated with the command and control of nuclear weapons. (Source: NSA/CSS Corporate Policy Glossary)

42. (U) Privileged Access (PRIVAC) – A special access above those privileges required for the normal data acquisition or operation of an agency information system. PRIVAC is granted to the following types of users:

a. (U) Users having "super-user," "root," "administrator," or equivalent special access to a system (e.g., systems administrators, computer system operators, system security officers, webmasters). Those individuals who have near or complete control of the operating system of the machine or information system, or who set up and administer user accounts, authenticators, and the like;

b. (U) Users who have been given the power to control and change other users' access to data or program files (e.g., application software administrators, administrators of specialty file systems, database managers, administrators);

c. (U) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and/or other important components; and

d. (U) Users who have been given special access for troubleshooting of information system security monitoring functions. (Source: PRIVAC website ("go privac"))

43. (U//~~FOUO~~) Second Party – Any of these countries: Australia, Canada, New Zealand, and the United Kingdom.

44. (U) Second Party Headquarters Personnel – Second Party personnel who work at Government Communications Headquarters (GCHQ), Communications Security Establishment (CSE), Australian Signals Directorate (ASD), or Government Communications Security Bureau (GCSB) headquarters or field elements and who have a valid need to access NSA/CSS classified ISs and for whom an NSA/CSS sponsor is identified.

45. (U//~~FOUO~~) Second Party Integree – Second Party personnel integrated into an NSA/CSS or United States Cryptologic System element who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct cryptologic or information assurance activities that support the NSA/CSS mission in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilian or military Second Party SIGINT or IA personnel but may not be contractors; an individual from one of the Second Party cryptologic entities assigned to work for NSA/CSS, under DIRNSA/CHSS authorities. Duties associated with an Integree's position shall be performed in support of the NSA/CSS mission and in compliance with Executive Order 12333, "United States Intelligence Activities," as amended. (Source: NSA/CSS Corporate Policy Glossary)

46. (U) Second Party Liaison Officers – A government official from a Second Party country, either military or civilian, who works in support of his or her country's objectives at a USG organization or installation. These individuals generally act as the immediate point of contact for official interaction between USG and the 2P for that geographic location. (Source: working definition, IC ITE and 5-Eyes Partner Fact Sheet, June 3, 2015)

47. (U) Service Partners – Those organizations with the five armed services that operate under Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) authority, or joint members of the larger Unified Cryptologic System, but that are not part of the CSS (e.g., Army Corps, Division, Separate Brigade and Armored Cavalry Regiment or Navy Fleet SIGINT assets that are normally under SIGINT Operational Tasking Authority (SOTA) of a tactical commander). (Reference j)

48. (U) System Security Plan (SSP) – The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. (Source: CNSSI 4009)

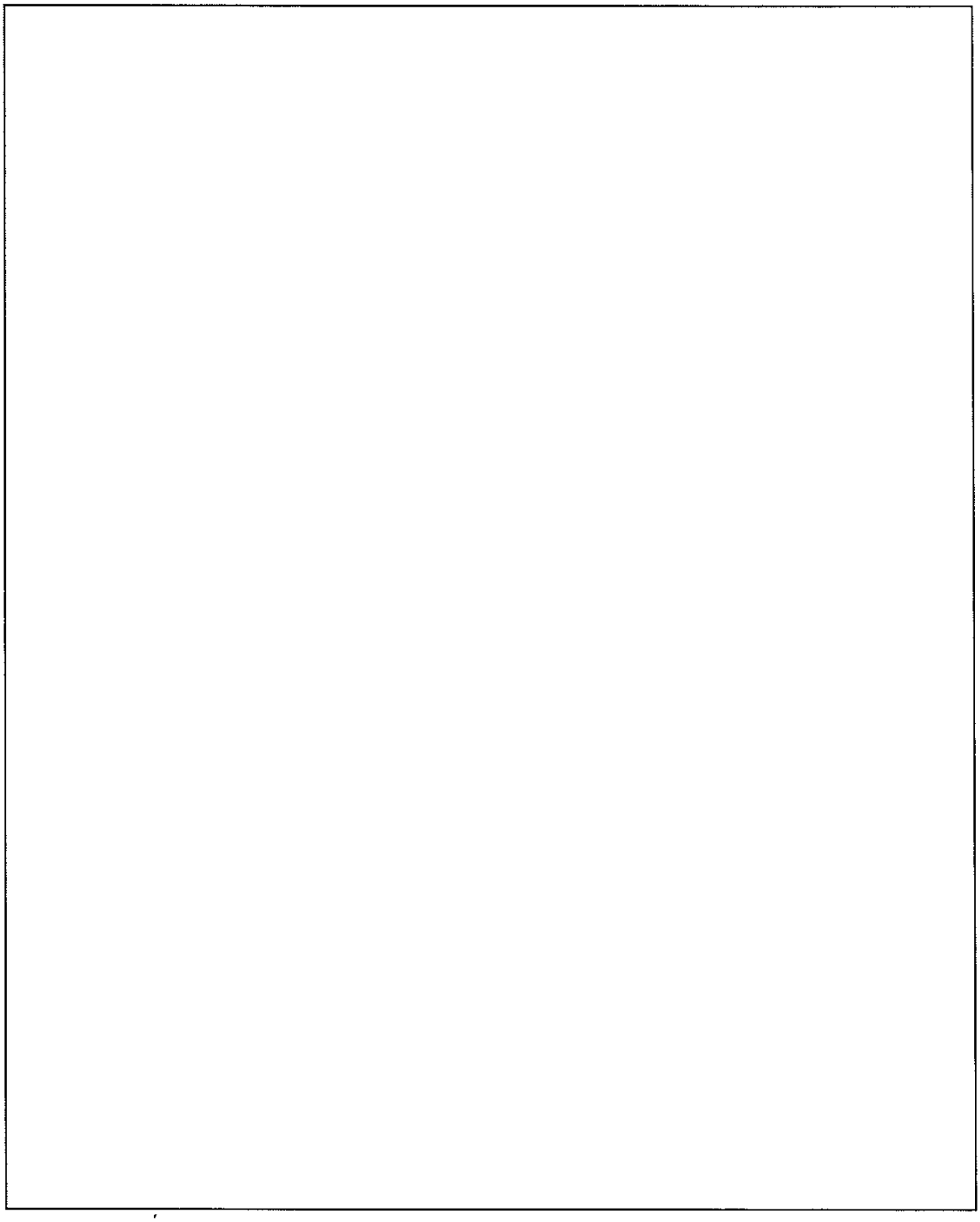
49. (U) United States Cryptologic System (USCS) – The various U.S. Government entities tasked with a SIGINT mission, i.e., the collection, processing, and dissemination of SIGINT, or with an information assurance mission, i.e., preserving the availability, integrity, authentication, confidentiality, and nonrepudiation of national security telecommunications and information systems. (Source: NSA/CSS Corporate Policy Glossary)

50. (U) USCS Personnel – United States Government personnel who derive their authority to direct and conduct cryptologic operations (SIGINT and IA) from the Director, NSA/Chief, CSS (DIRNSA/CHCSS). USCS Government personnel can be defined in three categories:

a. (U) Civilian employees of the National Security Agency;

b. (U) Military personnel and service civilians of the Service Cryptologic Components; and

c. (U) Military personnel and service civilians of the non-CSS military organizations and civilian integrees from other U.S. Intelligence Community agencies who are considered members of the USCS when performing SIGINT or IA operations under the direction, authority, and control of DIRNSA/CHSS. (Source: NSA/CSS Corporate Policy Glossary)



(b)(3)-P.L. 86-36